FORESIGHT

A PUBLICATION OF THE KENTUCKY LONG-TERM POLICY RESEARCH CENTER NO. 43 2005

A Year of CAN-SPAM, a Year of More Spam

This article assesses the efficacy of the federal CAN-SPAM Act of 2003, which, among its chief stipulations, prohibits e-mail address harvesting and requires bulk e-mailers include opt-out opportunities in their messages. Over the course of 11 months, the e-mail addresses we created for this study received over 11,000 pieces of spam, primarily due to illegal harvesting. Furthermore, 52 percent of these messages either lacked opt-out provisions or included nonfunctional opt-out mechanisms. Opting-out actually resulted in more spam: by the end of the year, addresses that opted-out received more than three times as much spam as addresses that never responded. Because the federal legislation has shown no discernible progress in reducing the volume of spam sent, savvy use of technology offers the current best hope for reducing the quantity of spam computer users receive. The FTC declined to establish a national do-not-spam registry, fearing the likelihood that unscrupulous spammers would exploit it as a ready-made list of "live" e-mail addresses. Nonetheless, some states, including Michigan and Utah, are moving forward with plans for state registries. The results of our experiment suggest the FTC made the prudent choice. Though the CAN-SPAM Act overrode state anti-spam laws, policymakers are urged to investigate the drafting of state laws that complement the federal legislation, such as an Iowa law that allows Internet Service Providers to claim $10 for each piece of illegal spam received, plus punitive damages. The prevalence of spam is ultimately driven by the high-profit, low-investment nature of bulk e-mailing, which rapidly became a common means of identity theft and bank fraud in 2004. Removing the financial incentive of unsolicited bulk e-mail will be key to solving this expensive epidemic.

By Mark Schirmer

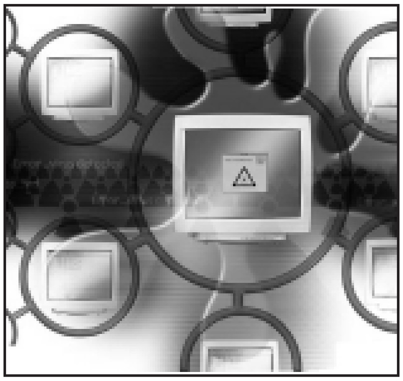
According to the United Nations' International Telecommunications Union, spam, or, more precisely, unsolicited bulk e-mail (UBE), "drains national economies around the world of about $25 billion a year and ... (the cost of) lost productivity … could be four times that amount."[1] In the United States alone, businesses lose about $22 billion a year in lost productivity due to UBE.[2] To stem the tide of spam, an increasing number of industrialized nations have enacted legislation to enable the prosecution and punishment of spammers. But in spite of these assorted laws, e-mail servers around the globe continue to be flooded with billions of spam messages, and the United States remains the world's top source of UBE.[3]

On January 1, 2004, the federal Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act went into effect. The law did not prohibit the sending of UBE. Rather, it stipulated that from this day forward such e-mails must contain opt-out options, valid postal addresses, warning labels for sexually explicit content, and accurate sender information, subject lines, and product claims. The Act also made illegal the unauthorized use of another's computer to send bulk e-mails and banned the harvesting of e-mail addresses from Web sites and mail servers.

Last July, we published a six-month progress report on CAN-SPAM that indicated the legislation had done nothing to diminish the onslaught of UBE up to that point in time. In this one-year assessment of CAN-SPAM's effect, we find that in spite of the growing number of criminal and civil cases against spammers, the volume of UBE transmitted globally has not abated and the content has grown increasingly malicious. Our discussion underscores the continued and emerging threats facing policymakers, technologists, and consumers, outlining some of the current measures to address these ongoing challenges.

Spam

Bulk e-mailers need not have high success rates to rake in huge profits, amply demonstrated in the recent trial of Jeremy Jaynes—not regarded as a particularly sophisticated spammer—who was sentenced to nine years in prison for peddling a bogus money-making program and masking return e-mail addresses. At his peak, Jaynes sent at least 10 million e-mails a day, 24 hours a day. Only about one in 30,000 e-mails (0.003 percent) resulted in a sale, but he earned roughly $40 per sale. All told, Jeremy Jaynes grossed between $400,000 and $750,000 *per month*, with only about $50,000 going for overhead expenses. Prosecutors estimated his net worth to be upwards of $24 million.[4] Though he amassed a sizable fortune, Jaynes' profits are the proverbial tip of the iceberg.



In a study commissioned by the Business Software Alliance and conducted by Forrester Data, 1,000 Internet users in the United States were surveyed on their experiences and attitudes regarding spam. Altogether, 41 percent of Americans surveyed stated they

Mr. Schirmer is a Research Assistant with the Center.

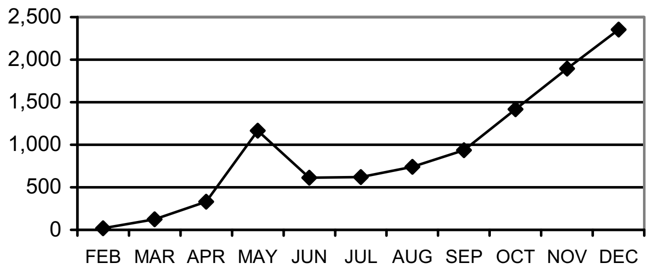
had bought something peddled in UBE.[5] Considering an estimated 75 to 82 percent of all e-mails are believed to be spam, that billions of e-mails are sent every month, and that a surprising portion of e-mail users actually take the bait, the staggering profits spammers pull in are the ultimate driving force behind the UBE epidemic.

Planting Seeds for E-Mail Harvesters

In February of 2004, after e-mail marketers had a month to adjust their tactics, the Kentucky Long-Term Policy Research Center created 12 e-mail accounts for the sole purpose of gathering illegal spam. We placed 11 of these addresses on several government Web sites, some hidden as comments within the HTML code, some hidden in plain sight by making the text the same color as the background; nine were created in plain text, two in ASCII.[6] (The 12th address was not listed anywhere online but could still receive e-mail.) Though invisible to the people visiting these pages, automated harvesters trawling the Internet for e-mail addresses would be able to find them.

In spite of the federal prohibition against harvesting, the hidden addresses began receiving e-mail only days after being posted online, and the influx steadily increased in the months to come. After anomalously spiking in May, the original trajectory resumed in June. In December 2004 alone, these addresses received over 2,300 e-mails; altogether they accumulated 11,371 pieces of spam in the span of 11 months (see Figure 1). ASCII code clearly made the harvesters' job tougher: these addresses received only 186 e-mails over the year, as opposed to the 1,678 received by the two comparison addresses in plain text.[7]

Figure 1: Number of Spam E-mails Received per Month, February to December 2004



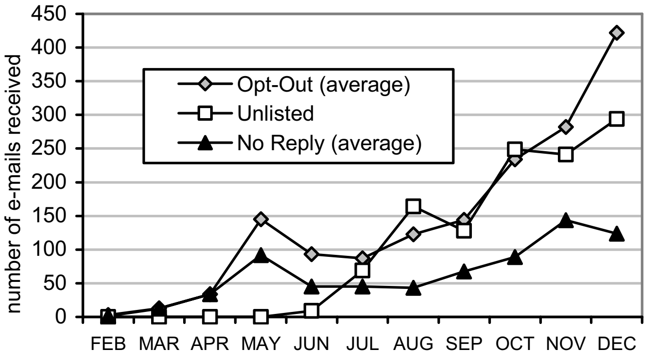
The Outcome of Opting-Out

Besides prohibiting harvesting, CAN-SPAM requires that spammers provide opportunities for recipients to opt-out of future e-mailings and that they in turn honor those requests. Even before the legislation went into effect, it came under criticism for not banning UBE outright.[8] Rather than require marketers to obtain opt-*in* requests before e-mailing in bulk—as do laws in Europe and Australia—the U.S. law permits spamming and places the onus of responsibility on the recipients of it, who are expected to contact spammers one by one with opt-out requests. Many predicted that opting out would only lead to more spam as such requests confirm the validity of an e-mail address. Our experiment tested that theory: four of the hidden addresses made opt-out requests to all the spam they received and a control set of four simply ignored the UBE.

The opt-out mechanisms in UBE generally entail either directions on how to submit opt-out requests via e-mail or hyperlinks to Web pages where recipients can go to submit their addresses for removal from e-mailing lists. If incoming messages contained either nonfunctioning Web links or no opt-out provisions, we e-mailed opt-out requests to the addresses of the apparent senders.

For the first three months, the *opt-out* and *ignore* addresses received nearly identical amounts of spam, but the two groups began to diverge dramatically in May, with the *opt-out* addresses receiving an increasing amount of spam. Over the course of the year the gap continued to grow, and in the last two weeks of December the *opt-outs* received over three times as much spam as the *ignores*. For the first four months, the *unlisted* address never received any e-mail, as it was not posted anywhere online and therefore could not be harvested. In June, however, the *opt-outs* started submitting the *unlisted* address in addition to their own addresses when utilizing Web-based opt-out mechanisms. Within three weeks, *unlisted* began to be spammed.[9] The volume of e-mail *unlisted* received exploded in July, exceeding the average received by the *ignores* each month thereafter and twice surpassing the *opt-outs*' average (see Figure 2). Clearly, opting out only assures a more crowded inbox.

Figure 2: The Outcome of Opting-Out



FORESIGHT
KENTUCKY
LONG-TERM POLICY RESEARCH CENTER
111 St. James Court, Frankfort, Kentucky 40601-8486
Phone: 502-564-2851 or 800-853-2851
Fax: 502-564-1412 or 800-383-1412
E-mail: info@kltprc.net
www.kltprc.net

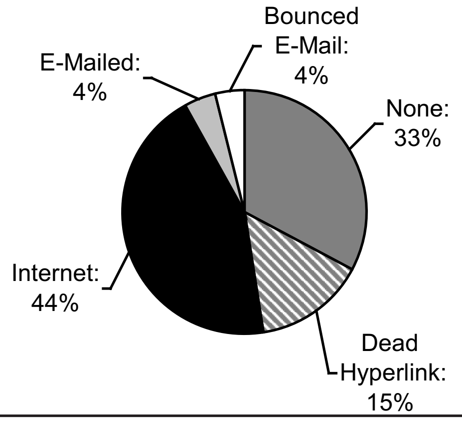
Layout
Suzanne King

Printed with state funds. Available in alternative formats upon request.

A Breakdown of Opt-Out Mechanisms

Of the e-mails received, 59 percent contained links to Web-based opt-out mechanisms, 8 percent instructed recipients to opt-out via e-mail, and the remaining 33 percent offered no opportunity of any kind.[10] One fourth of the Internet links went to dead pages, and 85 percent of the subsequent e-mailed requests were bounced as undeliverable. Among the spam with e-mail-based opt-outs, nearly 50 percent of the requests sent could not be delivered. In all, only 49 percent of all the e-mails contained functioning opt-out mechanisms (see Figure 3). Besides the fact that the study's e-mail addresses were obtained either through harvesting or through the opt-out mechanisms themselves, more than half of these spammers further violated CAN-SPAM either by not offering opportunities to opt-out or by not having functional opt-out mechanisms. Such problems typified spam in 2004: only about 3 percent of all UBE complied with CAN-SPAM guidelines.[11]

Figure 3: Opt-Out Mechanisms



Do-Not-E-Mail Registry and the Bounty System

At the behest of the CAN-SPAM legislation, the Federal Trade Commission investigated the viability of a national do-not-e-mail registry similar to the do-not-call registry that telemarketers must honor. The FTC found the proposed registry not to be feasible as the list of e-mail addresses could easily be abused by unscrupulous spammers. There are, however, a number of purported do-not-e-mail registries available online, some of which even cost money to join. Nevertheless, there's no such thing as a national do-not-e-mail list. The FTC warns that these alleged registries "may be a ruse to collect valid e-mail addresses to sell to spammers. The result could be even more spam for consumers who sign up for the 'registry.' Or, it may be even worse—some scammers have collected information through bogus Web sites that mimic those of legitimate organizations, and then use the information to commit identity theft."[12]

CAN-SPAM also called on the FTC to examine the possibility of formulating a bounty system to reward informants who identify lawbreaking spammers. That too came under fire from some anti-spam activists who feared it would encourage electronic vigilantism and would only help catch small-time operators.[13] It became a moot point in September when the FTC reported that "persons most likely to identify a spammer and provide evidence … (would be) personal or business associates of the spammers themselves," and that such whistle-blowers probably would be reluctant to step forward out of fear of being prosecuted themselves.[14] Without a do-not-e-mail registry or a viable bounty system, the effectiveness of the CAN-SPAM Act depends on spammers' willingness to offer and honor opt-out requests, and on the efficacy of the legislation as a tool for prosecuting lawbreakers.

Spam in the Courts

Because CAN-SPAM offers a legal remedy rather than a technological one, it can only stop spam insofar as spammers are either shut down through lawsuits and criminal convictions or deterred from continuing their practices by seeing what happens to those who get caught. Though only a drop in the bucket, this past year saw a handful of notable spam-related arrests and lawsuits in the courts, not all of which specifically invoked violations of the CAN-SPAM Act. In May, Howard Cormack, a.k.a. the "Buffalo Spammer," was sentenced to 3½ to 7 years in prison after being convicted of 14 counts of identity theft and forgery.[15] Yahoo! Inc. in June successfully sued a trio of Canadian spammers, who had to shut down their operation and pay at least $100,000 in damages.[16] Thanks to an Iowa law that allows Internet service providers to claim damages of $10 for each piece of illegal spam, plus punitive damages, Iowa-based CIS Internet Services was awarded a staggering $1 billion in a suit filed against three separate spamming companies.[17] Dozens more arrests were made and investigations initiated during 2004, and the results have begun to snowball.

In January 2005, Microsoft won a $7.4 million judgment against a spammer,[18] a federal judge granted a restraining order against six firms that failed to comply with CAN-SPAM's required labeling of sexually explicit e-mails,[19] the state of Texas sued two men identified as being among the world's top five spammers,[20] and Earthlink successfully sued and shut down the infamous "Alabama Spammers," who were also considered to be among the world's most prolific spammers. So far, none of these cases has made a noticeable dent in reducing the amount of spam sent globally.

Though the CAN-SPAM Act overrode existing state anti-spam laws, some state laws still exist that complement the federal legislation, such as the Iowa law that allowed CIS Internet Services to claim its massive settlement. Policymakers might consider investigating possibilities for state legislation that can piggyback onto the federal law to stiffen penalties against criminal spammers. To maximize the success of these legal actions, the authorities need evidence. The FTC has set up an e-mail address (spam@uce.gov) to which people are encouraged to forward the illegal spam they receive. Information garnered from this spam can then be added to a database used in the investigation and prosecution of lawbreaking spammers. Though the arrests and lawsuits will doubtlessly continue to pile up in 2005, spam will likely remain a massive problem for quite some time.

What Else Can Be Done?

Posting an e-mail address online—no matter how obscure the location—virtually guarantees it will be found by harvesters. Though the risk can be reduced by using ASCII in the HTML code, spammers have proven to be highly adaptive, so the advantage of ASCII will likely be nullified as harvesting software becomes more sophisticated. Others have suggested "munging" addresses, substituting numbers and symbols for letters: "name@domain" becomes "n@m3@d0m@!n."[21] That might go over in chat rooms and on message boards, but it would look unprofessional on business and government sites. One clever new technique has emerged that might be the only way to post e-mail addresses online so that they fool harvesters without appearing unprofessional: posting pictures of the addresses. Rather than typing the address in plain text or encoding it in ASCII, create a picture file—a jpeg or gif, for example—that displays it. Harvesters will have no way of decoding it, but human eyes won't have any trouble.

As we explained in last summer's *Policy Note* on spam, an increasing number of Web sites offer disposable e-mail addresses, which enable a single user to have multiple addresses, with all incoming messages forwarded to a single address. When one disposable address begins to receive spam, shut it down and create another disposable address. Because disposable e-mail addresses probably aren't feasible for businesses and government agencies, it's important that people reserve their professional e-mail accounts for professional purposes only. Separating business and recreation reduces the demands placed on an organization's computer resources, freeing them for their intended usage.[22]

For now, using e-mail filters remains the most effective tactic for unclogging inboxes. So far, however, programmers have yet to craft a filter that blocks all spam and allows all legitimate e-mail to pass through. Those employing e-mail filters must regularly monitor their spam folders for false positives, legitimate e-mails mistakenly flagged as spam. Furthermore, spammers adapt quickly and can modify their tactics in as little as five minutes after a filter has been updated.[23] Because so much UBE *is* successfully blocked, spammers have also increased the amount they send in order to maintain their sales. Though by no means a solution to the amount of spam *sent*, e-mail filters go a long way toward minimizing the quantity *received*.

Mutating and Malicious

A good deal of UBE seeks to sell products or services—a mere nuisance for most recipients—but a growing proportion of it exists solely for the commission of crime. Last year, UBE took great strides in its transformation from pest to threat as virus programmers, spammers, and organized crime integrated their efforts with immense success. In 2003, an average of 1 in 33 e-mails contained a virus; in 2004, it was 1 in 16.[24] Most of these viruses either commandeered control of PCs to turn them into "zombies" that would in turn send more spam, or implanted Trojan horses on machines that would gather sensitive personal data from computer users, such as bank account information and credit card numbers.[25] These problems have spread pervasively thanks to the self-propagating nature of viruses and the increasing usage of automated hacking.

Rather than spend time manually searching the Internet for vulnerable systems, automated hacking programs—"bots"—scan servers 24 hours a day, looking for machines to turn into zombies or infect with Trojan horses, and the process of downloading these pernicious programs can take as little as six seconds.[26] In 2003, computer security specialists had identified 750 *known* bot programs; that number grew to 2,300 by August of 2004.[27] Carnegie Mellon University's CERT® Coordination Center began keeping track of hacking incidents in 1988 when it recorded six attacks. It counted more than 20,000 attacks in 2000, over 130,000 in 2003, and in 2004—due to the prevalence of automated hacking—it stopped counting altogether.[28]

Whether infected by an e-mail attachment or by a bot, once a computer has been compromised hackers can control it remotely, renting it out to spammers by the hour. The pattern has evolved into the cyber-crime circle of life: programmers create viruses, hackers use the viruses to control personal computers, hackers rent the zombies to spammers, spammers hire programmers to create better viruses. This plague of zombies shows no sign of relenting: an estimated 80,000 to 100,000 PCs are converted to spam zombies *every week*, making it much easier for spammers to hide their tracks by sending UBE from other people's computers.

The Phishing Epidemic

Besides the proliferation of viruses and the zombie plague, another significant development in the evolution of spam was seen last year in the rapid emergence of "phishing," the practice of sending e-mails purportedly from institutions such as banks, credit card companies, and online retailers that direct recipients to "spoofed" Web sites where they're tricked into divulging financial information. In addition to violating the CAN-SPAM Act, phishers are also guilty of some combination of identity theft, wire fraud, credit card fraud, bank fraud, and computer fraud.[29] Toward the end of 2003, the Anti-Phishing Working Group (APWG)—an international consortium of law enforcement agencies, technology companies, and financial institutions—began tracking phishing attacks, each of which might be sent to numerous recipients. They recorded 28 unique attacks in November 2003[30] and 13,141 in February of 2005, a growth of nearly 47,000 percent.[31]

In July 2004, APWG began keeping tabs on active phishing sites. That month, they found 584 sites operating; three months later, nearly twice as many active sites were online; three months after *that*, the number had doubled again. The rapid rise seen since autumn has been attributed to new software that became available in October 2004 which enables the easy construction of phishing sites.[32] The toolkit allows new phishers to enter the fray and experienced phishers to expand their operations. By the end of last year, over 1,700 phishing Web sites were up and running; in January 2005, that number increased to 2,560, a 50 percent jump in just one month. Over one third of these sites are hosted in the United States.[33]

Like traditional spammers, phishers display a knack for being slippery. Phishing sites stay online for an average of less than one week, with life spans ranging from mere hours to one month, and it doesn't take long for them to be profitable. Once the recipient takes the bait and gives out the requested information, the data can be used to max out credit cards, open credit card and checking accounts, or be sold on the black market to those who wish to do the above. Approximately 5 percent of phishing recipients have been tricked into divulging financial information, with resulting losses estimated to be somewhere between $500 million and $2.4 billion.[34] Not surprisingly, identity theft has been the FTC's most-reported fraud complaint for the past five years.[35]

Fighting Phish

Some developers of anti-spam and anti-virus technology have added the creation of anti-phishing software to their workload, but because phishing e-mails so closely resemble legitimate corporate e-mails, the filters have an uphill battle. As large financial institutions fortify themselves against these scams, phishers have turned their attention to spoofing smaller, regional banks "whose customers may be less attuned to the threat."[36] And as e-mail users have grown increasingly wary of messages from banks and credit card companies—even when they're legitimate—"phishers have started mimicking power companies … trying to trick people into registering at fake utility Web sites to pay their bills automatically online.”[37] While programmers work to develop phishing filters, institutions that conduct electronic financial transactions—be they banks, retailers, or utility companies—must make a concerted effort to educate their customers about their e-mailing practices, reducing the likelihood they’ll get hooked by phishers.

The fallout from phishing has already grabbed the attention of policymakers. Last year, President Bush signed into law the Identity Theft Penalty Enhancement Act (ITPEA), under which those who use identity theft for the commission of other crimes can be prosecuted for “aggravated identity theft,” which carries a mandatory two-year prison sentence.[38] Additionally, Senator Patrick Leahy (D-Vermont) introduced the Anti-Phishing Act of 2004 last August which, if made law, would criminalize every step of the phishing process—regardless of whether the phishers’ efforts prove successful—and those convicted would face five years in prison and/or a fine up to $250,000.[39] As anti-phish legislation and technology evolve, so will the strategies of phishers, and the skyrocketing quantity of these messages sent each month will further burden already congested e-mail servers worldwide.

Looking Ahead

While concern over viruses has focused on the threats to PCs, hackers have begun targeting other products that use computer technology, such as cell phones, Blackberrys, and iPAQs. The Cabir worm, unleashed last year, actively seeks out devices that utilize Bluetooth technology, which uses radio connections to allow portable devices to communicate with one another. A Bluetooth cell phone can actually become infected with the Cabir worm merely by passing within 30 feet of a Bluetooth phone carrying the virus.[40] In 2002, roughly 35.8 million Bluetooth chipsets hit the market, and that number is expected to increase 74 percent each year through 2007. What’s more, over half the new cell phones sold in 2005 will utilize Bluetooth technology.[41] But the threat of viruses doesn’t stop with PCs, cell phones, and wireless devices. IBM recently warned that future viruses will begin infecting embedded computers, such as those controlling automobile functions and satellite communication systems,[42] though these claims have been hotly contested.[43]

A Refocused Vision

Because a national do-not-e-mail registry and a bounty system—two components of the CAN-SPAM Act—are either dead in the water or not terribly promising, the federal legislation will need to be revisited and retooled. Last August, the FCC ruled to prohibit the sending of unsolicited messages to wireless messaging services unless recipients have specifically opted-in.[44] Yet the law governing e-mailed spam still requires recipients to opt-out. Fax spam has been outlawed, in part because recipients wind up absorbing the cost of toner and paper to print documents they have not requested. Yet due to UBE, businesses and government agencies lose billions in productivity and spend billions on e-mail filtering software and services, thus absorbing the cost of receiving electronic documents they have not requested. Given the absence of a do-not-e-mail registry, the escalating costs of UBE paid for by its recipients, the mounting evidence that opting-out actually increases spam, and the opt-in provision already governing wireless spam, the time is ripe for policymakers to reconsider CAN-SPAM’s opt-out orientation.

Requiring e-mail marketers to obtain opt-in requests before sending out messages would not make spam disappear. Indeed, no law has ever precluded the commission of a crime. But questions of whether UBE contains valid postal addresses, opt-out Web links, or misleading subject lines aren’t at the heart of the spam problem. What matters most is that these e-mails are *unsolicited* and *bulk*, and the people sending them pay only a miniscule fraction of the total cost absorbed by the rest of the economy. That’s precisely why California, Australia, and the European Union enacted opt-in-oriented anti-spam laws. Future predictions of victory over spam might eventually prove to be more than wishful thinking, but success will be achieved only through a confluence of improved technology, savvy consumerism, and enhanced legislation.

Notes

[1] “Web Spam Can Be Beaten in Two Years, Say Regulators,” *ITWeb*, 7 July 2004, ITWeb Limited, 7 July 2004 <http://www.itweb.co.za/sections/internet/2004/0407070923i.asp>.

[2] Anick Jesdanun, “Deleting Spam Costs Billions, Study Finds,” *San Francisco Chronicle* 2 Feb. 2005, 3 Feb. 2005 <http://sfgate.com/cgi-bin/article.cgi?file=/n/a/2005/02/02/financial/f182339S36.DTL>.

[3] “The ‘Dirty Dozen’ 2004: Sophos Reveals the Top Spamming Countries,” *Sophos*, 24 Dec. 2004, Sophos Plc, 6 Jan. 2005 <http://www.sophos.com/spaminfo/articles/dirtydozenyear.html>.

[4] “Trial Shows How Spammers Operate,” *MSNBC*, 15 Nov. 2004, Microsoft Corporation, 4 Feb. 2005 <http://www.msnbc.msn.com/id/6492244/>.

[5] “Consumer Attitudes Toward Spam in Six Countries,” *Business Software Alliance*, 9 Dec. 2004, Business Software Alliance, 16 Dec. 2004 <http://www.bsa.org/usa/events/loader.cfm?url=/commonspot/security/getfile.cfm&pageid=20654>. The survey’s margin of error was ±3 percent.

[6] The plain text addresses appeared in readily understandable language: “name@domain.” ASCII addresses can be read by machines only. For example, “name@domain” would appear in the HTML code as “&#110;&#97;&#109;&#101;&#64;&#100;&#111;&#109;&#97;&#105;&#110;.” We also hyperlinked some of these addresses to see if the HTML code for e-mail hyperlinks (<a href=“mailto:name@domain”>) would attract more spam, but saw no discernible effect.

[7] Of the two ASCII addresses, one was hyperlinked and one was not. Neither responded to any of the spam they received, and both were masked by making the font the same color as the Web page’s background. To gauge the effect of using this code, we compared the volume of UBE received by these two addresses with the volume received by a control pair of plain text addresses, neither of which responded to spam, one of which was hyperlinked, and both of which were colored to blend into the background. In other words, they were alike in every way except for whether we created them in ASCII or plain text. The total number of e-mails received by these four addresses represents a subset of the total received during the course of our study.

[8] Anita Ramasastry, “Why the New Federal ‘CAN SPAM’ Law Probably Won’t Work,” *CNN.com*, 5 Dec. 2003, Cable News Network, 14 Feb. 2005 <http://www.cnn.com/2003/LAW/12/05/findlaw.analysis.ramasastry.spam>.

[9] The *unlisted* address never submitted opt-out requests of any kind.

[10] A negligible 0.167 percent contained telephone numbers to call with opt-out requests. These numbers were always functional and required the caller to leave a message on an answering machine, spelling out the e-mail address to be removed.

[11] George V. Hulme, “A Look at the Law: Can the Government Have an Impact on Spyware?” *Information Week* 17 Jan. 2005: 62.

[12] United States, Federal Trade Commission, “Keep Your Email Address *Un*listed: There Is No ‘National Do Not Email Registry,’” Aug. 2004, 3 Feb. 2005 <http://www.ftc.gov/bcp/conline/pubs/alerts/dnealrt.htm>.

[13] Mike Brunker, “FTC Mulls Bounty System to Combat Spammers,” *MSNBC*, 30 June 2004, 30 June 2004 <http://www.msnbc.msn.com/id/5326107/>.

[14] United States, Federal Trade Commission, “FTC Assesses Reward System for Catching Spammers,” 16 Sep. 2004, 3 Feb. 2005 <http://www.ftc.gov/opa/2004/09/bounty.htm>.

[15] “‘Buffalo spammer’ sentenced to 3½ to 7 years,” *Forbes.com*, 27 May 2004, Forbes.com Inc., 4 Feb. 2005 <http://www.forbes.com/newswire/2004/05/27/rtr1387102.html>.

[16] “Canadian spam king relinquishes throne,” *MSNBC*, 15 June 2004, 7 Feb. 2005 <http://www.msnbc.msn.com/id/5214929/>.

[17] Grant Gross, "Internet Service Provider Awarded $1 Billion in Spam Damages," *PCWorld.com*, 20 Dec. 2004, PC World Communications, Inc., 16 Feb. 2005 <http://pcworld.com/news/article/0,aid,119011,00.asp>.

[18] Scott Simonson, "Microsoft: 'Spammer' in Tucson Owes $7.4M," *Arizona Daily Star* 1 Jan. 2005, 4 Feb. 2005 <http://www.dailystar.com/dailystar/relatedarticles/55002.php>.

[19] Laurie Kellman, "FTC Targets Porn Spammers," *CBSNews.com*, 11 Jan. 2005, CBS Broadcasting Inc., 4 Feb. 2005 <http://www.cbsnews.com/stories/2005/01/11/>.

[20] "Texas sues major spam operation," *CNN.com*, 14 Jan. 2005, 18 Jan. 2005 <www.cnn.com/2005/TECH/internet/01/14/texas.spam.lawsuit.reut/>.

[21] "Crabby's Top 10 Spam-Fighting Tips," *Microsoft Office Online*, 2004, Microsoft Corporation, 1 Mar. 2005 <http://office.microsoft.com/en-us/assistance/HA010701261033.aspx>.

[22] Mark Schirmer, "The CAN-SPAM Act of 2003: A Six-Month Progress Report," *Policy Notes* July 2004: 2.

[23] Katie Hafner, "Delete: Bathwater. Undelete: Baby.," *New York Times on the Web* 5 Aug. 2004, 6 Aug. 2004 <http://www.nytimes.com/2004/08/05/technology/circuits/05filt.html>.

[24] Thomas Claburn, "Machine Wars," *Information Week* 17 Jan. 2005: 57.

[25] An increasing proportion of these viruses and Trojans are spread via instant messaging rather than e-mail.

[26] Claburn 56.

[27] Claburn 56.

[28] "CERT/CC Statistics 1988-2004," *CERT Coordination Center*, 2005, Carnegie Mellon University, 2 Feb. 2005 <http://www.cert.org/stats/cert_stats.html>.

[29] United States, Department of Justice, "Special Report on 'Phishing,'" Mar. 2004, 2 Feb. 2005 <http://www.usdoj.gov/criminal/fraud/Phishing.pdf>.

[30] "Phishing Activity Trends Report: April, 2004," *Anti-Phishing Working Group*, May 2004, Anti-Phishing Working Group, 15 Feb. 2005 <http://www.antiphishing.org/APWG_Phishing_Attack_Report-Apr2004.pdf>.

[31] "Phishing Activity Trends Report: February, 2005," *Anti-Phishing Working Group*, 24 Mar. 2005, 29 Mar. 2005 <http://www.antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf >.

[32] "Phishing Activity Trends Report: October, 2004," *Anti-Phishing Working Group*, Nov. 2004, 15 Feb. 2005 <http://antiphishing.org/APWG_Phishing_Activity_Report-Oct2004.pdf>.

[33] "Phishing Activity Trends Report: January, 2005," *Anti-Phishing Working Group*, 24 Feb. 2005, 25 Feb. 2005 <http://www.antiphishing.org/APWG_Phishing_Activity_Report-January2005.pdf>.

[34] Ross Wehner, "Phishers Threaten E-Commerce," *E-Commerce Times*, 1 Jan. 2005, ECT News Network, Inc., 3 Feb. 2005 <http://www.ecommercetimes.com/story/39306.html>.

[35] Bob Sullivan, "ID theft tops list of FTC complaints," *MSNBC*, 1 Feb. 2005, 2 Feb. 2005 <http://www.msnbc.msn.com/id/6891556/>.

[36] Brian Krebs, "Phishers Drop Hooks into Smaller Streams," *Washington Post* 24 Jan. 2005, 2 Feb. 2005 <http://www.washingtonpost.com/wp-dyn/articles/A32199-2005Jan24.html>.

[37] Krebs.

[38] Anita Ramasastry, "Hooking Phishermen," *CNN.com*, 16 Aug. 2004, 3 Feb. 2005 <http://www.cnn.com/2004/LAW/08/16/ramasastry.phishing/>.

[39] Ramasastry, "Hooking Phishermen."

[40] George V. Hulme, "Dial V for Virus," *Information Week* 6 Dec. 2004: 19.

[41] George V. Hulme, "Bluetooth: Handy, but worrisome," *Information Week* 6 Dec. 2004: 20.

[42] "Surge in Viruses and Worms Targeting Mobile Devices, Satellite Communications Anticipated in 2005," *IBM Press Room*, 9 Feb. 2005, IBM, 14 Feb. 2005 <http:/www.ibm.com/press/PressServletForm.wss?>.

[43] Matt Hines, "Lexus slams brakes on in-car virus theory," *Silicon.com* 18 Feb. 2005, CNET Networks Inc., 18 Feb. 2005 <http://software.silicon.com/malware/0,3800003100,39127957,00.htm>.

[44] "FCC Bans Wireless Spam," *Mobile Pipeline*, 5 Aug. 2004, CMP Media LLC, 3 Feb. 2005 <http://www.mobilepipeline.com/showArticle.jhtml?articleID=26806070>.

Public Forums Suggest Worsening Problems with Access to Health Care

By Michal Smith-Mello

Health insurance has become increasingly unaffordable for a substantial portion of Kentuckians, most on hand for a series of public forums held by the Kentucky Health Insurance Research Project asserted. Held in each of the state's 15 Area Development Districts (ADDs), the forums are part of a federally funded initiative being conducted by the University of Kentucky (UK), the Kentucky Long-Term Policy Research Center, and the University of Louisville (UL). They were designed to gather information about the scope of the problem and the underlying causes of uninsurance in the Commonwealth and inform the larger project.

A common theme emerged from the forums: cost and access to health care are huge problems in our state as in the nation as a whole. The sentiments echo those found in a series of national polls which have found health care at the top of a long list of issues of critical concern. A November 2004 Employee Benefit Research Institute poll, for example, found that Americans are as concerned about health care as they are about national security and terrorism. Similarly, Gallup has long found that two thirds of Americans view the U.S. system as having major problems or being in crisis.

Those in attendance cited low earnings and the rising cost of health insurance as the main reasons why more than half a million Kentuckians are estimated to be without health insurance. That gap, research consistently shows, often deters people from getting the health care they need when they need it, a situation that many in attendance reported as being all too commonplace.

Health care providers consistently observed that the county-level estimates of the uninsured population presented in the forums were too low to capture the magnitude of the problem. Estimates presented were based on county-level data from the Lewin Group, a national health care research organization, and on population projections from the State Data Center.

In the majority of forums, providers in attendance reported that the number of uninsured is growing, and only "Band-aids" exist to help with their care. As a result, many are going without the care they need, having to choose basic necessities over life-sustaining medications or treatments, and, in too many instances, dying or becoming disabled as a consequence of their inability to afford needed health care.

Just behind them, others testified, are the underinsured or what social scientist Rose Weitz terms the "precariously insured," those whose financial well-being will be devastated by a health incident *or* who will not be able to sustain coverage over the long term. This population, these forums suggest, could be as large as or larger than those who are completely without health insurance. With co-insurance costs or deductibles as high as 25 percent, a single high-tech test leaves low-wage earners struggling financially for months. An insured western Kentucky woman recounted the financial strain one unnecessary CAT scan had placed on her and her family. Many do not recover.

A Harvard University study recently found the results are too often "medical bankruptcy"; that is, a precipitating medical event ultimately leads to the loss of health insurance, followed by unmanageable medical expenses, the loss of savings and assets, and, ultimately, bankruptcy. A bankruptcy attorney at a central Ken-

Ms. Smith-Mello is a Senior Policy Analyst with the Center and Project Director for the Kentucky Health Insurance Research Project.

tucky public health forum reported that as many as 70 percent of his clients had become bankrupt due to health care expenses, losing virtually everything they had worked for all their lives in the process.

Perhaps at greatest risk are older Kentuckians who are not yet old enough to qualify for Medicare. Some retired early, often for health reasons; others lost jobs in industries that have moved offshore and were forced to take marginal jobs. Due to their ages and health conditions, some of which are treatable, many are being priced out of the insurance market, or the coverage they can afford leaves them exposed to considerable financial risk.

J.D. Miller, Vice President of Medical Affairs for Appalachian Regional Healthcare makes a point at the Hazard forum at the University of Kentucky Center for Rural Health, as David L. Long (left), Director of Human Resources for Red Bird Mission and Red Bird Clinic, and Joel Medendorp, Director of Health and Wellness for Red Bird Clinic, look on.

Photo by David A.Gross, UK Center for Rural Health

Input from the forums also suggests that the high cost of health insurance is taking a toll on community institutions. Officials of small cities, hospitals, nonprofit, and charitable organizations, small and mid-sized businesses, some health departments, and other community institutions reported a succession of double-digit premium hikes. As a result, employers and officials in attendance reported that they would soon have to cut employees, reduce current health care benefit levels, or both.

In the case of those small cities opting to buy insurance on the private market, officials reported that quality benefit packages help them retain employees. Fire and police protection, in particular, were cited by some small city mayors and officials as areas where employee losses can be particularly costly, given the extent of investment in training. If health insurance costs continue to escalate, a range of public services could be undermined, particularly in communities adjoining border states that offer higher entry-level wages.

Hospitals report being in a double bind. They not only face rising costs for insuring their own employees but continue to absorb higher and higher costs for charity or uncompensated care. One Appalachian hospital official said that charity care costs had doubled at the hospital she represented in the first half of the past fiscal year. Hospital officials openly acknowledged that the costs of that care are being shifted to the privately insured and to Medicare. Medicaid reimbursements, it was generally agreed among these officials, fails to meet actual costs, presenting yet another financial problem for these community institutions.

In the absence of readily available community health centers or free clinics, both of which are woefully inadequate in number to meet needs in Kentucky, uninsured people often turn to an emergency department (ED) where they cannot be turned away for care. But EDs are the least efficient means of providing primary care, a key cost driver identified by a number of those in attendance at the forums. What's more, by the time many reach the ED, their conditions have become far more advanced, more debilitating, and more costly to treat.

On a brighter side, hospital officials often reported that they offer uninsured and low-income patients sliding-scale fees for care, but acknowledged that the uninsured had to seek such assistance in order to become aware of it. Only one individual out of more than 215 in attendance reported having negotiated his own fees for needed medical tests while being uninsured. More typically, the uninsured tend to be financially stressed, undereducated, often isolated and without transportation, wary of seeking treatment for fear of the burden it would pose for them and their families, and generally ill-equipped to negotiate the "system."

Providers in attendance also reported that insurers in the state routinely delay reimbursement; deny certain diagnostic tests outright, regardless of the reason for the test; and routinely delay credentialing for six months. As a result, newly hired doctors—some in underserved areas—cannot be reimbursed for work that otherwise would be covered until the insurer satisfies its own credentialing requirements.

Providers at every forum reported that the administrative costs associated with navigating the varying health insurance plans are high and quite burdensome. One London physician quipped that he would make more money if he only treated uninsured people and charged them $25 for an office visit.

And input at these forums suggests that some of the protections intended to shield people from becoming uninsured or being hurt as a consequence are not working. COBRA benefits are reportedly too costly for the unemployed, the displaced worker, or the individual who develops an illness after leaving the security of a job. Kentucky Access, the state's high-risk pool designed to extend insurance to individuals with certain conditions whose insurance has been cancelled, was cited as an unaffordable avenue for many by those in attendance. A Lexington woman, who acknowledged that she numbered among those lucky enough to be able to afford monthly premiums that rose fourfold after she developed cancer, asked rhetorically how a family or individual of modest means could hope to meet such costs.

Some providers reported that Medicaid's safety net has become frayed in Kentucky; the provider network is inadequate, and eligibility requirements more cumbersome. For the undereducated and the poor, who often live with relatives or friends out of necessity and do not have access to dependable transportation, requiring recipients to provide receipts on a monthly basis presents an obstacle to coverage. These individuals, providers report, are clearly eligible; they simply cannot prove it. And, even if they could, many who attended the forums reported that few physicians in their area were willing to take Medicaid patients.

Programs run by pharmaceutical companies to provide low-income individuals with needed medications are not readily accessible to the poor and uneducated. Many are simply unaware of them. And, without advocates or ready access to a computer, others cannot meet what are reportedly constantly changing eligibility requirements. One Hazard-based charitable organization reported dedicating significant staff time to negotiating these programs to get medications for the uninsured people they help.

Finally, these forums suggest that issues related to under- and uninsurance clearly affect the state's economic well-being, inhibiting labor participation and worker productivity, and raising societal costs for carrying a large uninsured population. Further, the monthly premiums for health insurance reported in these forums were so substantial, even for relatively healthy people, that the costs likely cut deeply into the disposable incomes of many, given the state's comparatively low wages and salaries, the continued movement of jobs offshore, and persistent pockets of high unemployment. Ironically, the choice to buy health insurance, these forums suggest, leaves many Kentuckians without the economic capacity to buy the very goods and services that drive our economy and, in turn, generate tax revenues.

The Kentucky Health Insurance Research Project is funded by a federal state planning grant from the Federal Health Resources and Services Administration, which facilitates state-level responses to the problems of the uninsured. The UK Center for Rural Health is spearheading the work in partnership with the Kentucky Long-Term Policy Research Center, a state agency, and the UL Center for Excellence in Urban Health. A multidisciplinary team from these institutions is studying the scope of the problem through large- and small-group meetings; statewide surveys of the general population and small businesses, which are far less likely to provide health insurance; and an analysis of the economic cost of uninsurance. Importantly, the project will analyze policy options available to the state and propose strategies for increasing the insured population.

Nominations for the 2005 Vic Hellard, Jr. Award given each year at the Center's annual conference are now being accepted. Forms are available at http://www.kltprc.net//hellardaward.htm.

The deadline for nominations is September 9, 2005.

Scanning Kentucky

Beginning with this issue, *Scanning Kentucky* will be a part of *Horizon*, which will showcase emerging trends, issues, ideas, and innovations. We invite readers to participate by collecting information from print, online, radio or television reports, speeches, or public opinion polls that offers a glimpse of the future; then pass it along to us via fax, mail, e-mail, or our Web site. We will synthesize and summarize the information for review by our Board and publish selected items. We hope that citizens will become involved to help shape a better future for our state. To contribute to *Horizon* or receive further information, please visit http://www.kltprc.net/scan/scanentry.htm on the Center's Web site or contact Billie S. Dunavent.

Mark your calendar for the Center's 12th Annual Conference to be held at the Louisville International Convention Center, November 15, 2005.